Deutscher Bundestag **Drucksache 18/9388**

18. Wahlperiode 11.08.2016

Antwort
der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Dr. Alexander S. Neu, Jan van Aken, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/9221 –

Sogenannte hybride Bedrohungen und deren tatsächliche Gefährlichkeit

Vorbemerkung der Fragesteller

Am 6. April 2016 veröffentlichten die Europäische Kommission und der Europäische Auswärtige Dienst ihre Initiative „Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen, die Stärkung der Resilienz der EU, ihrer Mitgliedstaaten und Partnerländer und den Ausbau der Zusammenarbeit mit der NATO bei der Bekämpfung solcher Bedrohungen“. Ein entsprechendes Papier enthält Vorschläge für 22 operative Maßnahmen (JOIN(2016) 18 final). Laut einer am gleichen Tag herausgegebenen Pressemitteilung seien die Europäische Union (EU) und ihre Mitgliedstaaten „in zunehmendem Maße hybriden Bedrohungen ausgesetzt“. Das Sicherheitsumfeld habe sich drastisch verändert, auch an den Außengrenzen der EU nähmen „hybride Bedrohungen“ zu. „Hybride“ Aggressionen würden nicht nur unmittelbaren Schaden anrichten und Verwundbarkeiten ausnutzen, sondern Gesellschaften destabilisieren und „durch Verschleierungstaktik“ die Entscheidungsfindung zu einer gemeinsamen Antwort behindern. Innere und äußere Sicherheit müssten deshalb noch stärker miteinander verknüpft werden. Auch Geheimdienste sollen sich an der Abwehr von „hybriden Angriffen“ unterhalb der Schwelle militärischer Gewalt beteiligen.

Im September 2015 rief der Europäische Auswärtige Dienst ein Team für „Strategische Kommunikation“ (EU EAST STRATCOM) ins Leben, um damit die politischen EU-Ziele in der östlichen Nachbarschaft „voranzutreiben“ (Bundestagsdrucksache 18/6486). Die Arbeitsgruppe soll „Desinformationskampagnen über den Ukrainekonflikt“ kontern. Inzwischen hat die EU zahlreiche Folgedokumente und Strategien zu „hybriden Bedrohungen“ veröffentlicht. Die Bundesregierung bestätigt jedoch, dass solche „hybriden Bedrohungen“ in Deutschland bislang nicht festzustellen sind. Allenfalls würden „Desinformations- und Propagandamaßnahmen“ beobachtet.

Der Begriff der „hybriden Bedrohungen“ ist nicht eindeutig begrifflich definiert. Als Beispiel gilt der Einsatz verdeckt operierender oder nicht gekennzeichneter Spezialkräfte bei „gleichzeitigem Aufbau einer konventionellen militärischen Drohkulisse“. Die Europäische Kommission schreibt von einer „Vermischung militärischer und ziviler Kriegsführung durch staatliche und nichtstaatliche Akteure wie verdeckte Militäroperationen, intensive Propaganda und wirtschaftliche Drangsalierung“ (https://ec.europa.eu/germany/

Die Antwort wurde namens der Bundesregierung mit Schreiben des Auswärtigen Amts vom 9. August 2016 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

news/eu-verst%C3%A4rkt-antwort-auf-hybride-bedrohungen_en). Ziel sei dabei nicht nur, unmittelbaren Schaden anzurichten und Verwundbarkeiten auszunutzen, „sondern auch Gesellschaften zu destabilisieren und durch Verschleierungstaktik die Entscheidungsfindung zu behindern". Dies trifft nach Ansicht der Fragesteller aber genauso auf die Kriegsführung im Jemen, in Syrien oder Libyen zu, insbesondere auch auf die Aufstandsbekämpfung der US-Regierung in den 80er-Jahren in Lateinamerika.

Trotz der vagen Begriffsbestimmung sind nun konkrete Maßnahmen geplant. Das Lagezentrum EU Intelligence and Situation Centre (EU INTCEN) in Brüssel soll eine „Hybrid Fusion Cell" eröffnen. Die Zelle erstellt Frühwarnberichte und arbeitet mit anderen Agenturen zusammen. Genannt werden die bei Europol angesiedelten Zentren gegen Cyberkriminalität sowie gegen Terrorismus, die Grenzschutzagentur Frontex und das Computersicherheits-Ereignis- und Reaktionsteam der EU (CERT-EU). Schließlich soll die „Hybrid Fusion Cell" ein Abkommen mit der Abteilung gegen „hybride Bedrohungen" bei der NATO schließen. Anvisiert sind unter anderem gemeinsame Übungen „auf politischer und technischer Ebene". Auch die Bundeswehr will mit militärischen und zivilen Mitteln zur „Krisenfrüherkennung" reagieren.

1. In welchen EU- oder NATO-Mitgliedstaaten ist das tatsächliche Vorkommen allgemeiner „hybrider Bedrohungen" aus Sicht der Bundesregierung derzeit zu beobachten?

Westliche Demokratien mit ihren offenen pluralistischen Gesellschaften bieten vielfältige Angriffsflächen und sind damit in besonderem Maße durch hybride Aktivitäten verwundbar. In dieser Hinsicht können sämtliche EU- und NATO-Mitgliedstaaten zum Ziel hybrider Kampagnen werden. Wie stark ein Staat jeweils betroffen ist, hängt davon ab, wie sehr er im Fokus staatlicher und nichtstaatlicher Akteure steht, die zur Erreichung ihrer Ziele den koordinierten Einsatz verschiedenster ziviler und militärischer Mittel und Instrumente nutzen. Der Bundesregierung liegen darüber hinaus keine weiteren eigenen Erkenntnisse zu dieser Frage vor.

2. Inwiefern teilt die Bundesregierung die Einschätzung der EU-Gruppe „Politisch-militärische Angelegenheiten", wonach eine „Cyberdimension" bei „hybriden Bedrohungen" unter anderem in der Ukraine und einigen EU-Mitgliedstaaten zu beobachten sei (Ratsdokument 9701/16; bitte die aus Sicht der Bundesregierung eingetretenen „Bedrohungen" benennen)?

In der Ukraine konnte nach der Majdan-Revolution eine auffällige Zunahme des Eindringens in IT-Systeme beobachtet worden. Zudem hat im Dezember 2015 ein Cyberangriff zu einem Ausfall von Teilen des ukrainischen Stromnetzes geführt. Ein einschlägiger Fall in Deutschland war der Angriff auf Websites verschiedener Bundesministerien im Januar 2015. Für andere EU-Mitgliedstaaten liegen der Bundesregierung keine eigenen Erkenntnisse zu dieser Frage vor. Ergänzend wird auf die Antwort zu Frage 1 verwiesen.

3. Mit welchen Maßnahmen wird die Bundesregierung die „Schlussfolgerungen des Rates zur Bewältigung hybrider Bedrohungen“ vom 19. April 2016 (Ratsdokument 7928/16) berücksichtigen und/oder umsetzen, der ein „rasches und angemessenes Handeln zur Prävention und Bewältigung von hybriden Bedrohungen für die Union und ihre Mitgliedstaaten sowie für ihre Partner“ anmahnt?

Innerhalb der Bundesregierung wurden in den Ressorts, in deren Zuständigkeit mögliche Einzelmaßnahmen zur Abwehr komplexer hybrider Bedrohungen liegen, Kopfstellen benannt, die im Eventualfall eine schnelle gesamtstaatliche Reaktion ermöglichen sollen. Innerhalb dieses Netzwerks wird derzeit die Position der Bundesregierung zu den Einzelmaßnahmen erarbeitet.

4. Wann sollen Details zur Umsetzung dieser Maßnahmen vorliegen bzw. inwiefern befinden sich diese weiterhin in der „ressortübergreifende[n] Ableitung der Bundesregierung“ (Bundestagsdrucksache 18/8631)?

Die ressortübergreifende Ableitung ist noch nicht abgeschlossen. Auf die Antwort zu Frage 3 wird verwiesen.

5. Inwiefern sieht sich die Bundesregierung weiterhin lediglich „Desinformations- und Propagandamaßnahmen“ und keinen belegbaren „hybriden Bedrohungen“ ausgesetzt (Bundestagsdrucksache 18/8631)?

Die Bewertung der Bundesregierung in der in Bezug genommenen Antwort hat weiterhin Bestand. Der Bundesregierung liegen aktuell keine Erkenntnisse für den Einsatz darüber hinausgehender hybrider Mittel in Deutschland vor. In diesem Zusammenhang stellt die Bundesregierung klar, dass sie gemäß ihrer Definition der hybriden Austragung von Konflikten auch Propaganda und Desinformation als Elemente eines „hybriden Szenarios“ und damit als Teilaspekte hybrider Bedrohungen betrachtet (Auf die Antwort der Bundesregierung zu den Fragen 1 und 6 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/8631 vom 1. Juni 2016 wird verwiesen).

6. Inwiefern hält die Bundesregierung Cyberangriffe nicht für ein „denkbar[es]“ Mittel hybrider Konfliktaustragung, sondern konnte diese tatsächlich als „hybride Bedrohungen“ werten?

Aus Sicht der Bundesregierung sind Cyberangriffe der verschiedensten Ausprägungen ein geeignetes Mittel hybrider Konfliktaustragung und damit auch Element einer hybriden Bedrohung. Auf die Antwort zu Frage 2 wird verwiesen.

7. Welche Vorkehrungen trifft die Bundesregierung zur Abwehr eines hypothetischen „großangelegten, schweren hybriden Angriffs“, der laut Bundestagsdrucksache 18/8631 zwar nicht zu erwarten ist, aber auch nicht grundsätzlich ausgeschlossen werden kann?

Die Unterbindung und Abwehr hybrider Angriffe erfordert eine wirksame ressortgemeinsame und gesamtstaatliche Sicherheitsvorsorge. Diese beinhaltet vor allem die frühzeitige Aufklärung einer hybriden Bedrohung sowie die Stärkung von Resilienz.

8. Wann liegen der Bundesregierung Details zu der geplanten „Hybrid Fusion Cell“ im geheimdienstlichen EU-Lagezentrum INTCEN in Brüssel vor, bzw. inwiefern hat sie seit ihrer Antwort auf Bundestagsdrucksache 18/8631 vom 1. Juni 2016 versucht, diese Details zu erfragen?

Der EU-Analyseeinheit für hybride Bedrohungen („EU Hybrid Fusion Cell“) ist mittlerweile eingerichtet worden.

a) Inwiefern wurde die für Juni 2016 geplante Inbetriebnahme der „Hybrid Fusion Cell“ tatsächlich umgesetzt (Ratsdokument 9701/16)?

Die EU-Analyseeinheit für hybride Bedrohungen („EU Hybrid Fusion Cell“) hat im EU-Zentrum für Informationsgewinnung und -analyse des Europäischen Auswärtigen Dienstes am 26. Juni 2016 die so genannte Erste Einsatzfähigkeit („Initial Operational Capability“) hergestellt.

b) Was ist der Bundesregierung mittlerweile über die (geplanten) Tätigkeiten der „Hybrid Fusion Cell“ bekannt?

Aufgabe der EU-Analyseeinheit für hybride Bedrohungen ist es, dem Europäischen Auswärtigen Dienst, der Kommission, dem Rat und den EU-Mitgliedstaaten Analysen zu hybriden Bedrohungen zur Verfügung zu stellen.

c) Welche In- oder Auslandsgeheimdienste oder sonstigen Beteiligten sollen dieser „Hybrid Fusion Cell“ angehören?

Der EU-Analyseeinheit für hybride Bedrohungen gehören Angehörige des Europäischen Auswärtigen Dienstes an.

d) Inwiefern soll die neue „Hybrid Fusion Cell“ auch Internetbeobachtung betreiben, und wer würde auf diese Weise beobachtet?

Die EU-Analyseeinheit für hybride Bedrohungen analysiert Informationen aus offenen Quellen, darunter das Internet.

e) Welche Aufgaben werden dort von welchen Behörden übernommen?

Die EU-Analyseeinheit für hybride Bedrohungen erstellt Berichte über die Existenz möglicher hybrider Bedrohungen, die gegen einen Mitgliedstaat, Partnerstaaten oder -organisationen gerichtet sind. Der Direktor des EU-Zentrums für Informationsgewinnung und -analyse wird den Stellvertretenden Generalsekretär für die Gemeinsame Sicherheits- und Verteidigungspolitik und Krisenmanagement im Europäischen Auswärtigen Dienst, den Stellvertretenden Generalsekretär in der Europäischen Kommission sowie die EU-Ratspräsidentschaft unterrichten. Diese werden dann Vorschläge zum weiteren Vorgehen für die Hohe Vertreterin, den Präsidenten der Europäischen Kommission, die EU-Ratspräsidentschaft und den Präsidenten des Europäischen Rates erstellen.

f) Was ist der Bundesregierung über geplante Zusammenarbeitsformen dieser „Hybrid Fusion Cell“ mit der NATO bekannt?

Die am 8. Juli 2016 in Warschau verabschiedete Gemeinsame Erklärung des Präsidenten des Europäischen Rates, des Präsidenten der Europäischen Kommission und des NATO-Generalsekretärs sieht mit Blick auf hybride Bedrohungen eine

verstärkte Kooperation in den Bereichen Informationsaustausch und – soweit möglich – Austausch relevanter nachrichtendienstlicher Erkenntnisse sowie bei der strategischen Kommunikation vor. Zudem sollen die Verfahren beider Organisationen zum Umgang mit hybriden Bedrohungen aufeinander abgestimmt werden. Zur Umsetzung werden EU und NATO auf Arbeitsebene bis Jahresende Mechanismen zur Interaktion und Koordinierung ausarbeiten.

g) Inwiefern hat die „Hybrid Fusion Cell“ mittlerweile Abkommen mit der NATO-Abteilung gegen „hybride Bedrohungen“ geschlossen?

Nach Kenntnis der Bundesregierung wurden bisher keine solchen formalen Vereinbarungen getroffen.

h) Inwiefern stehen mittlerweile Einzelheiten dazu fest, bei welcher Behörde bzw. Abteilung die Bundesregierung eine nationale Kontaktstelle für die „Hybrid Fusion Cell“ einrichten wird?

Einzelheiten zur Einrichtung einer nationalen Kontaktstelle der Bundesregierung für die EU-Analyseeinheit für hybride Bedrohungen stehen noch nicht fest. Hierzu läuft die Abstimmung zwischen den zuständigen Ressorts der Bundesregierung.

9. Mit welchen „diesbezüglich relevanten EU-Gremien“ sollte die „Hybrid Fusion Cell“ aus Sicht der Bundesregierung kooperieren (Bundestagsdrucksache 18/8631)?

Die EU-Analyseeinheit für hybride Bedrohungen sollte insbesondere mit den anderen Arbeitseinheiten des Europäischen Auswärtigen Dienstes und der Europäischen Kommission kooperieren. Darüber hinaus ist ein enger Informationsaustausch mit den EU-Mitgliedstaaten von besonderer Bedeutung.

a) Mit welchen Anstrengungen sind nach Kenntnis der Bundesregierung auch die Polizeibehörde Europol und die Grenzschutzagentur Frontex sowie der Ständige Ausschuss des Rates für die innere Sicherheit (COSI) hinsichtlich „hybrider Bedrohungen“ befasst?

Die Bundesregierung hat keine Erkenntnisse, inwiefern sich die Agenturen Europol und Frontex mit hybriden Bedrohungen befassen. Die Gemeinsame Mitteilung der Europäischen Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik „Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen“ vom 6. April 2016 nennt im Zusammenhang mit Ziffer 4.6 „Stärkung der Resilienz gegen Radikalisierung und gewalttätigen Extremismus“ die Arbeit der bei Europol angesiedelten EU-Meldestelle für Internetinhalte. Der Ständige Ausschuss für die operative Zusammenarbeit im Bereich der inneren Sicherheit hat in einer gemeinsamen Sitzung mit dem Politischen und Sicherheitspolitischen Komitee am 3. März 2016 das Thema „hybride Bedrohungen“ diskutiert.

b) Mit welchen Drittstaaten sollen Europol, Frontex und der COSI hierzu Kontakt aufnehmen (Ratsdokument 14636/15)?

Die Bundesregierung hat keine Erkenntnisse, mit welchen Drittstaaten Europol, Frontex oder der Ständige Ausschuss für die operative Zusammenarbeit im Bereich der inneren Sicherheit zum Thema hybride Bedrohungen Kontakt aufnehmen.

10. Welche gemeinsamen Übungen der „Hybrid Fusion Cell“ und der NATO sind nach Kenntnis der Bundesregierung derzeit „auf politischer und technischer Ebene“ geplant?

Gemäß der Gemeinsamen Erklärung des Präsidenten des Europäischen Rates, des Präsidenten der Europäischen Kommission und des NATO-Generalsekretärs vom 8. Juli 2016 ist für die Jahre 2017 und 2018 die Durchführung paralleler und aufeinander abgestimmter Übungen der NATO und der EU geplant. Konkrete Planungen liegen der Bundesregierung bislang nicht vor.

a) Welche Stäbe der EU und der NATO sind zur Ausformulierung von parallelen oder gemeinsamen Übungen „in engem Kontakt“?

In Kontakt stehen der Internationale Stab und der Internationale Militärstab der NATO sowie die EAD-Direktion Krisenbewältigung/Planung und der EU-Militärstab der EU.

b) Auf welche Weise unterstützt die Bundesregierung das „Vorhaben“ gemeinsamer Übungen?

Die Bundesregierung befürwortet die Durchführung gemeinsamer sowie paralleler und aufeinander abgestimmter Übungen und behält sich eine Beteiligung an den für die Jahre 2017 und 2018 geplanten Übungen vor.

11. Was ist der Bundesregierung über den Inhalt eines technischen Abkommens zwischen dem CERT-EU und dem NATO-Kommando „Computer Incident Response Capability“ hinsichtlich „hybrider Bedrohungen“ bekannt?

Bei der am 10. Februar 2016 unterzeichneten technischen Vereinbarung zwischen dem NATO-Reaktionsteam für Computersicherheit („Computer Incident Response Capability“ – NCIRC) und dem IT-Notfallteam der Europäischen Union (CERT-EU) handelt es sich um eine völkerrechtlich nichtbindende Absprache zum Austausch von Informationen und Erfahrungen. Gegenstand dieses Austauschs sind unter anderem Informationen über neue Bedrohungen im Cyberraum und den Umgang mit diesen Bedrohungen.

12. Was ist der Bundesregierung über eine „diplomatic toolbox“ hinsichtlich „hybrider Bedrohungen“ bekannt (Ratsdokument 6908/16)?

    Wer hat diese „toolbox“ entwickelt bzw. umgesetzt?

Der Bundesregierung ist kein diplomatischer Instrumentenkasten zu hybriden Bedrohungen bekannt.

Ein Instrumentenkasten für Cyber-Diplomatie wurde in den zuständigen EU-Gremien erarbeitet. Zweck des Instrumentenkastens für Cyber-Diplomatie ist es, in allgemeiner Form die nach den Unionsverträgen bestehenden Möglichkeiten zusammenzustellen, mit denen EU-Mitgliedsstaaten und die EU auf etwaige Cyberangriffe auch mit außenpolitischen Mitteln reagieren können.

13. Welche Aussagen trifft die „toolbox“ zur Frage, auf welche Weise betroffene oder unterstützende Staaten Cyberangriffe oder „hybride Bedrohungen“ auf politischer, diplomatischer, rechtlicher oder wirtschaftlicher Ebene beantworten sollen?

Auf die Antwort zu Frage 12 wird verwiesen. Der Instrumentenkasten für die Cyber-Diplomatie trifft keine Aussage zu der Frage, auf welche Weise betroffene oder unterstützende Staaten Cyberangriffe oder „hybride Bedrohungen“ im Einzelfall auf politischer, diplomatischer, rechtlicher oder wirtschaftlicher Ebene beantworten sollen.

14. Welche konkreten Maßnahmen trifft der in Wales 2014 beschlossene „Readiness Action Plan“ der NATO hinsichtlich „hybrider Konfliktszenarien“, zu denen der Bundesregierung zufolge „unter anderem asymmetrische Einsatzformen, Propaganda und Desinformation oder auch Cyberattacken und -sabotage und die Nutzung des Informationsraums“ gehören (Bundestagsdrucksache 18/8904)?

Der Plan für eine erhöhte Einsatzbereitschaft identifiziert Themenfelder, in denen eine Anpassung der NATO an das veränderte sicherheitspolitische Umfeld angezeigt ist. Er leistet auf diese Weise einen entscheidenden Beitrag, um dem Phänomen hybrider Bedrohungen in seinen militärischen Aspekten im Bündnisrahmen mit dem gesamten Spektrum an Instrumenten begegnen zu können. Dies beinhaltet die Schaffung und Anwendung von notwendigen Instrumenten und Verfahren für effektive Abschreckungsmaßnahmen und adäquate Reaktionen auf hybride Bedrohungen. Weiter zielt der Plan auf eine Verbesserung der strategischen Kommunikation, die Entwicklung von Übungsszenarien mit Bezug auf hybride Bedrohungen und eine Stärkung der Koordination zwischen der NATO und anderen internationalen Organisationen im Einklang mit den einschlägigen gefassten Beschlüssen.

a) Mit welchen Einzelmaßnahmen gehen auch eine „Strategie [der NATO] zum Umgang mit hybrider Kriegsführung“ und ein dazugehöriger Implementierungsplan auf „hybride Konfliktszenarien“ ein?

Die „Strategie zur Rolle der NATO beim Umgang mit hybriden Bedrohungen“ beschreibt die Rolle der NATO im Gesamtrahmen des sogenannten DIMEFIL-Spektrums („Diplomatic/Political, Information, Military, Economic, Financial, Intelligence, Legal“). Als langfristig angelegte Strategie benennt sie keine konkreten Einzelmaßnahmen.

Der Implementierungsplan operationalisiert die Strategie anhand verschiedener Arbeitsstränge. Dabei stehen die Steigerung der Aufklärungsfähigkeit, die Entwicklung eines Übungsprogramms sowie die Resilienzbildung im Mittelpunkt.

b) Auf welche Weise wird die Bundesregierung die Aufforderung der NATO an die Mitgliedstaaten zur Eigenverantwortung bei der „Resilienzstärkung“ bezüglich „hybrider Konfliktszenarien“ bzw. „hybrider Bedrohungen“ umsetzen?

Im Rahmen des am 13. Juli 2016 verabschiedeten Weißbuchs 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr hat die Bundesregierung staatliche und gesamtgesellschaftliche Resilienz als Grundvoraussetzung für eine erfolgreiche Prävention gegen hybride Gefährdungen benannt. Die Aussichten auf Erfolg

einer solchen Resilienzbildung werden durch diese effektive Vernetzung relevanter Politikbereiche wesentlich erhöht. Hierzu gehören ein besserer Schutz kritischer Infrastrukturen wie z. B. der Abbau von Verwundbarkeiten im Energiesektor, Fragen des Zivil- und des Katastrophenschutzes, eine wirksame Cyberabwehr, effiziente Grenzkontrollen, eine polizeilich garantierte innere Ordnung und schnell verlegbare, einsatzbereite militärische Kräfte.

Ein wichtiger Schritt zur Umsetzung wird dabei die von der Bundesregierung in Kürze zu beschließende neue Konzeption Zivile Verteidigung sein, auf deren Grundlage eine Präzisierung und Fortentwicklung der vorhandenen und benötigten Fähigkeiten vorgenommen sowie alle einschlägigen Rechtsgrundlagen auf die Notwendigkeit einer Fortentwicklung geprüft werden sollen.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333